Claims

1. Method for cryptographically processing a message, wherein - a first partial cryptographic key and a second partial cryptographic key, which correspond to a decomposition of a private cryptographic key, are used;
- the message is processed using the first partial cryptographic key resulting in a first partially processed message;
- the message is processed using the second partial cryptographic key resulting in a second partially processed message;
- the first partially processed message and the second partially processed message are combined resulting in a cryptographically processed message.

2. The method according to claim 1, wherein the processing of the message using the first partial cryptographic key is carried out by a first computer and the processing of the message using the second partial cryptographic key is carried out by a second computer.

3. The method according to claim 2, wherein the first and the second computer are coupled via a computer network.

4. The method according to claim 2 or claim 3, wherein the method further comprises the step of transmitting the message from the first computer to the second computer.

5. The method according to any of the claims 1 to 4, wherein the first partial cryptographic key and the second partial cryptographic key correspond to a

decomposition of the private cryptographic key into a plurality of partial cryptographic keys.

6. The method according to claim 5, wherein the plurality of partial cryptographic keys give, when summed, the private cryptographic key.

7. The method according to any of the claims 1 to 6, wherein the cryptographical processing of the message is the signing of the message or the decrypting of a message.

8. The method according to any of the claims 1 to 7, wherein the message is processed according to a public key cryptographic algorithm.

9. The method according to claim 8, wherein the public key cryptographic algorithm is the RSA algorithm.

10. The method according to any one of the claims 1 to 9 wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined.

11. The method according to claim 10, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

12. Computer system comprising
- a first processing unit which is adapted to process a message using a first partial cryptographic key, which

corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- a second processing unit which is adapted to process a message using a second partial cryptographic key, which corresponds to the decomposition of the private cryptographic key, resulting in a second partially processed message;
- a combining unit which is adapted to combine the first partially processed message and the second partially processed message resulting in a cryptographically processed message.

13. Method for generating a cryptographically processed message wherein
- a message is processed using a first partial cryptographic key, which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- the message is transmitted to a client computer;
- a second partially processed message is received which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key;
- the first partially processed message and the second partially processed message are combined to a cryptographically processed message.

14. Server computer comprising
- a processing unit which is adapted to process a message using a first partial cryptographic key, which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;

- a transmitting unit which is adapted to send the message to a client computer;
- a receiving unit which is adapted to receive a second partially processed message which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key;
- a combining unit which is adapted to combine the first partially processed message and the second partially processed message to a cryptographically processed message.

15. Method for performing a cryptographic operation on a message, wherein
- a message is received;
- the message is processed using a partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a partially processed message;
- the partially processed message is transmitted to a server computer.

16. Client computer comprising
- a receiving unit which is adapted to receive a message;
- a processing unit which is adapted to process the message using a partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a partially processed message;
- a transmitting unit which is adapted to transmit the partially processed message to a server computer.

17. Computer program element which, when executed by a computer, makes the computer perform the following steps

- processing a message using a first partial cryptographic key which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- processing the message using the second partial cryptographic key which corresponds to the decomposition of the private cryptographic key resulting in a second partially processed message;
- combining the first partially processed message and the second partially processed message resulting in a cryptographically processed message.

18. Computer program element which, when executed by a computer, makes the computer perform the following steps
- processing a message using a first partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a first partially processed message;
- transmitting the message to a client computer;
- receiving a second partially processed message which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key;
- combining the first partially processed message and the second partially processed message to a cryptographically processed message.

19. Computer program element which, when executed by a computer, makes the computer perform the following steps
- receiving a message;
- processing the message using a partial cryptographic key which corresponds to a decomposition of a private

cryptographic key resulting in a partially processed message;

- transmitting the partially processed message to a server computer.